Bolton Clinical Commissioning Group

Information Governance Policy

Policy Number	**IG001**
Target Audience	**CCG/CSU Staff**
Approving Committee	**CCG Executive**
Date Approved	**January 2014**
Last Review Date	**January 2016**
Next Review Date	**December 2017**
Policy Author	**Senior IG Officer (GMSS)**
Version Number	**V2.0**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	August 2013	M Robinson/ D Sankey	Progress to CCG Executive team for approval
1	August 2013	CCG Executive Team	Approved
1.1	January 2014	Andrea Hughes	Amendment to Section 5
	January 2014	IM&T Ops Board	Approved
1.2	November 2015	IG Team	Review document for approval
2.0	December	IM & T Ops	Approved

Analysis of Effect completed	By: M Robinson	Date: August 2013

Contents

1 Introduction and aims

1.1. This document sets out minimum policy standards and common policy directions across Bolton Clinical Commissioning Group for confidentiality, integrity and availability of information (Information Governance). The policy is intended to cover the overlapping areas of Data Protection Act 1998 compliance, Freedom of Information Act 2000 compliance, Information Security Management Systems (ISO 27001:2005), Data Quality and Confidentiality (with regard to 'common law').

1.2. Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service.

1.3. Information Governance sits alongside Clinical Governance, Research Governance and Corporate Governance. It provides a framework to bring together all of the requirements, standards and best practice that apply to the handling of personal information. It also provides a consistent way for employees to deal with the many different information handling requirements including:

- information governance management; clinical information assurance;
- confidentiality and data protection assurance;
- corporate information assurance; information security assurance; and secondary use assurance.

1.4. The aims of this document are to maximise the value of organisational assets by ensuring that data is:

- held securely and confidentially;
- obtained fairly and lawfully;
- recorded accurately and reliably;
- used effectively and ethically; and
- shared and disclosed appropriately and lawfully.

In order to protect the organisations information assets from all threats, whether internal or external, deliberate or accidental, the CCG will ensure:

- information will be protected against unauthorised access;
- confidentiality of information will be assured;
- integrity of information will be maintained;
- information will be supported by the highest quality data;
- regulatory and legislative requirements will be met;
- business continuity plans will produced, maintained and tested;
- information security training will be available to all staff; and
- all breaches of information security, actual or suspected, will be reported to, and investigated by, the GM Shared Services (GMSS) Information Governance Team.

1.5. This policy applies to those members of staff who are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience, the organisation's policies are also applicable whilst undertaking duties for or on behalf of the CCG. This policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

2 Information Governance Policy Framework

2.1. The Information Governance framework will be supported by a set of related policies and procedures to cover all aspects of Information Governance and which are aligned with the NHS Operating Framework and the Information Governance Toolkit requirements.

The Policy framework will encompass the following:

- Records Management Policy
- Corporate Information Security Policy
- Information Risk Policy
- Acceptable Use of IT & Equipment Policy (includes email & internet)
- Encryption Policy
- Confidentiality & Data Protection Policy

In addition, specific procedural documents will be part of the Information Governance suite of policies which will be supported by those framework documents, above.

This policy list is not exhaustive and changes in the organisation may lead to additional documents or changes to this list.

2.2. **Information Governance User Handbook**

An Information Governance user handbook/guide has been developed that provides a brief introduction to Information Governance and summarises the key user requirements that support the CCG Information Governance policies.

3 Information Governance Group

The CCG has established an Information Governance Group, to monitor and co-ordinate with service suppliers the implementation and ongoing management of the Information Governance framework and IG Toolkit requirements.

4 Information Governance Team

4.1. The Information Governance Team will be provided by GMSS and supply expert advice and guidance to all staff on all elements of Information Governance. The team is responsible for:

- Information Governance Framework

- Information Asset Register – Management and Support
- IG Toolkit
- IG Training
- IG Policies
- IG Administration
- Compliance Support
- Support Senior Information Risk Officer and Caldicott Guardian

4.2. The Information Governance Team will be steered by the CCG Information Governance Group, the CCG Caldicott Guardian and the SIRO, within the structure of the contractual arrangements that exist between the CCG and GMSS for the provision of IG services.

4.3. The Information Governance Group will report to the Caldicott Guardian and CCG Executive Team and this will also be the route of escalation for issues.

5 Accountability, Responsibilities and Training

5.1 The Chief Officer has ultimate responsibility for the implementation of the provisions of this policy. As the 'Accountable Officer' they are responsible for the management of the organisation and for ensuring that the appropriate mechanisms are in place to support service delivery and continuity.

The CCG has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of and compliance with internal and external governance requirements

5.2. Responsibilities will be delegated to:

A Caldicott Guardian who will:

- ensure that the CCG satisfies the highest practical standards for handling patient identifiable information;
- act as the conscience of the CCG;
- facilitate and enable information sharing and advise on options for lawful and ethical processing of information;
- represent and champion Information Governance requirements and issues at Board level;
- ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff;
- oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS.

A Senior Information Risk owner (SIRO) will:

- be an Executive Director or Senior Management Board Member;
- take overall ownership of the Organisations Information Risk Policy
- act as champion for information risk on the Board and provide advice to the Accounting Officer on the content of the Organisation's

Statement of Internal Control in regard to information risk;

- understand the strategic business goals of the CCG and how other NHS organisations' business goals may be impacted by information risks, and how those risks may be managed;
- work with GMSS (supplier of IG) to manage the NHS Information Governance risk assessment and management processes within the CCG;
- advise the Board on the effectiveness of information risk management across the CCG;
- receive training as necessary to ensure they remain effective in their role as SIRO.

Information Asset Owners (IAO) will:

- lead and foster a culture that values, protects and uses information for the success of the CCG and benefit of its customers;
- know what information comprises or is associated with the asset, and understand the nature and justification of information flows to and from the asset;
- know who has access to the asset, whether system or information, and why, and ensure access is monitored and compliant with policy;
- understand and address risks to the asset, and providing assurance to the SIRO.

Information Governance Supplier, GMSS will:

- manage the Information Governance Team to deliver Information Governance for the CCG;
- maintain an awareness of information governance issues within the CCG;
- review and update the information governance policy in line with local and national requirements providing template documents to the CCG;
- ensure that line managers are aware of the requirements of the Information Governance policy.

5.3 Line managers will take responsibility for ensuring that the Information Governance Policy is implemented within their staff group or directorate, including any temporary or contract staff.

It is the responsibility of each employee to adhere to the policy.

Staff will receive instruction and direction regarding the policy from a number of sources:

- policy/strategy and procedure manuals;
- line manager;
- specific training course;
- other communication methods, for example, team meetings; and staff Intranet.

All individuals (including any temporary or contract staff) will be required to comply with this policy whilst working within the CCG and thereafter for as long as the information remains confidential information.

All staff (including any temporary or contract staff) are mandated to undertake the "Introduction to Information Governance" e-learning module. Information Governance training is required to be undertaken on an annual basis. The CCG will decide where relevant further training and education will be required of staff. Staff will be informed via the Information Governance Training Needs Analysis.

6 Monitoring and review

6.1. This policy will be monitored through staff awareness and supporting evidence to the NHS IG Toolkit

6.2. This Policy will be reviewed on an annual basis, and in accordance with the following, on an as and when required basis:

- legislative changes;
- good practice guidance;
- case law;
- significant incidents reported; new vulnerabilities; and
- changes to organisational infrastructure.

7 Legislation

Information will be defined and where appropriate kept confidential, underpinning the principles of the Caldicott Report 1997 and the legal requirements of the Data Protection Act 1988, the Human Rights Act 2000 and in keeping with the Common Law Duty of Confidentiality.

8 Other relevant Procedural Documents

8.1 A set of Procedural Documents will be made available via the CCG Intranet.

- IG009 Confidentiality Audit Procedure
- IG013 Subject Access Procedure
- RA Procedure
- IG007 Incident Management Procedures
- IG012 Secure Transfer of Information Procedure

This list is not exhaustive

8.2 Staff will be made aware of procedural document updates as they occur via team briefs, team meetings and notification via the CCG staff intranet.

8.3 A number of other policies in the General Policy/Strategy Manual are related to this policy and all employees will be made aware of the full range.